An Underground Education

Lessons in Counterintelligences from History's Underworld

@thegrugq

Agenda

- Counterintelligence
  - Processes
  - Threats
  - Contributing Factors
- Professional Thieves: CI
- Hackers: CI

Counterintelligence

Processes of CI

- Basic Denial
- Adaptive Denial/Insight
- Covert Manipulation

- Prevent the transfer of information to the adversary
- Primarily proscriptive
  - Don’t engage in some behavior
- Enough for basic survival

- OPSEC
  - STFU
- COMSEC
- Vetting members to prevent penetrations

examples

The first breach of security occurs when the opposition becomes aware that information worthy of targeting exists.

Counterintelligence: Theory and Practice

After the adversary knows there is something to look for, then the game begins. You can’t go back underground. :(

- Insight into oppositions techniques/processes
  - Develop countering tactics
- Analyze security posture for weaknesses
  - Develop remediations
- Ongoing process

Dual pronged approach. On the one hand, learn how the adversary works and attempt to work around those strengths/capabilities
On the other, look at organisational weaknesses and address them.
Iterative. Best if there is a penetration into the adversary to monitor how they function

- Adjust to remedy unique vulnerabilities and/or adversarial strengths
- Greatly benefits from access to adversarial know-how
- Active penetrations of the adversary are very useful here

Colombian narco traffickers used court discovery heavily to discover the Tactics, Techniques and Procedures of the adversary
The PIRA started to do the same thing later in their struggles, forcing the .gov to reveal details

Covert Manipulation

- Provide the adversary with false information
  - Deceive the adversary into taking futile action
  - Deceive the adversary into not taking action
- Mostly irrelevant for hackers
  - Misdirection could be valuable, maybe.

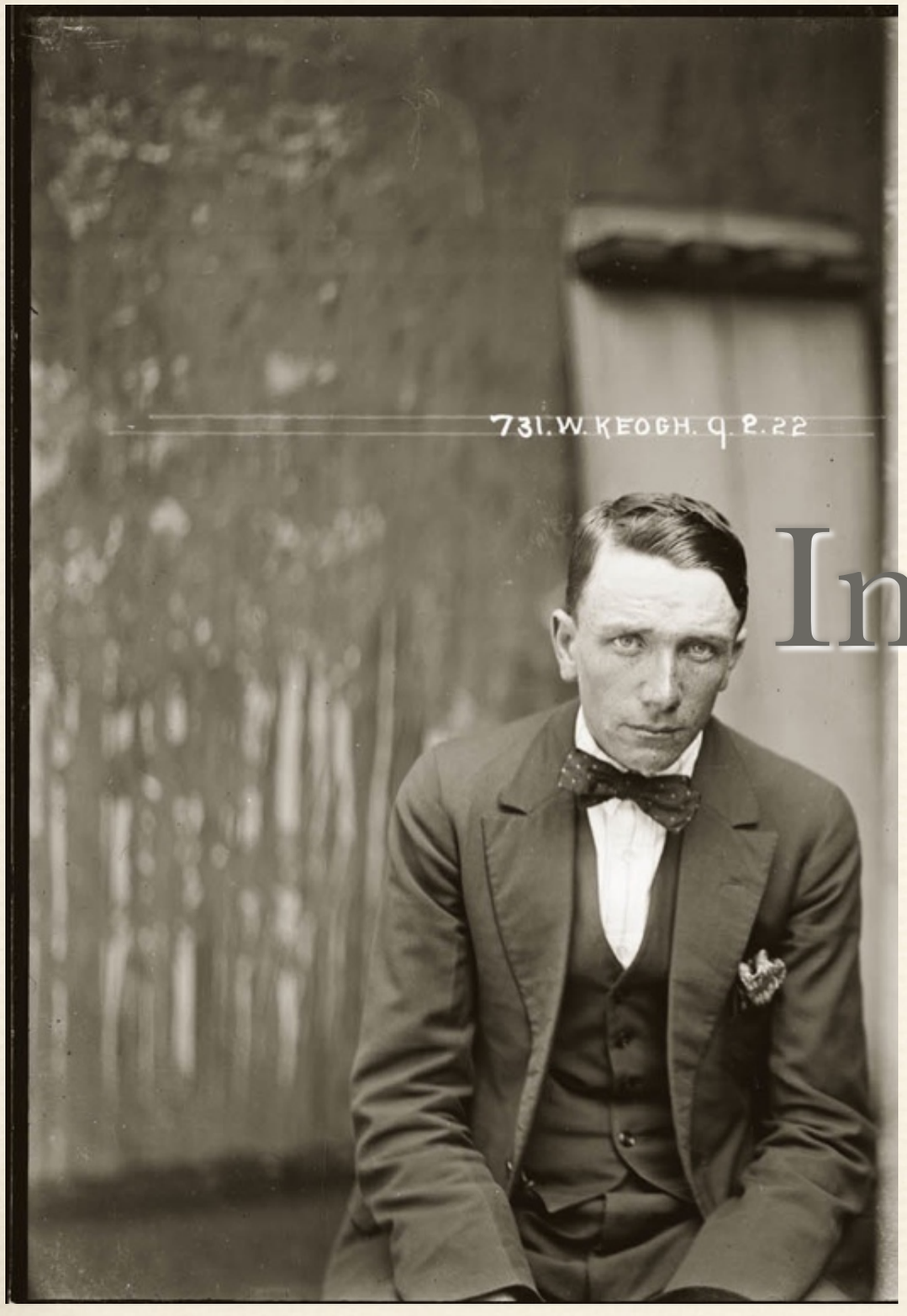
Adversary has multiple channels for receiving information, have to send fake signals down them all. HUMINT, technical penetrations, open source INT, etc. etc.

Intelligence Threats

The capabilities of the adversary are described as “intelligence threats”, that can be used to gain information about the agency.

- Penetrations
- Technical Penetrations
- Passive Surveillance
- Media Exposure

HUMINT, SIGINT, ... OSINT



Informants

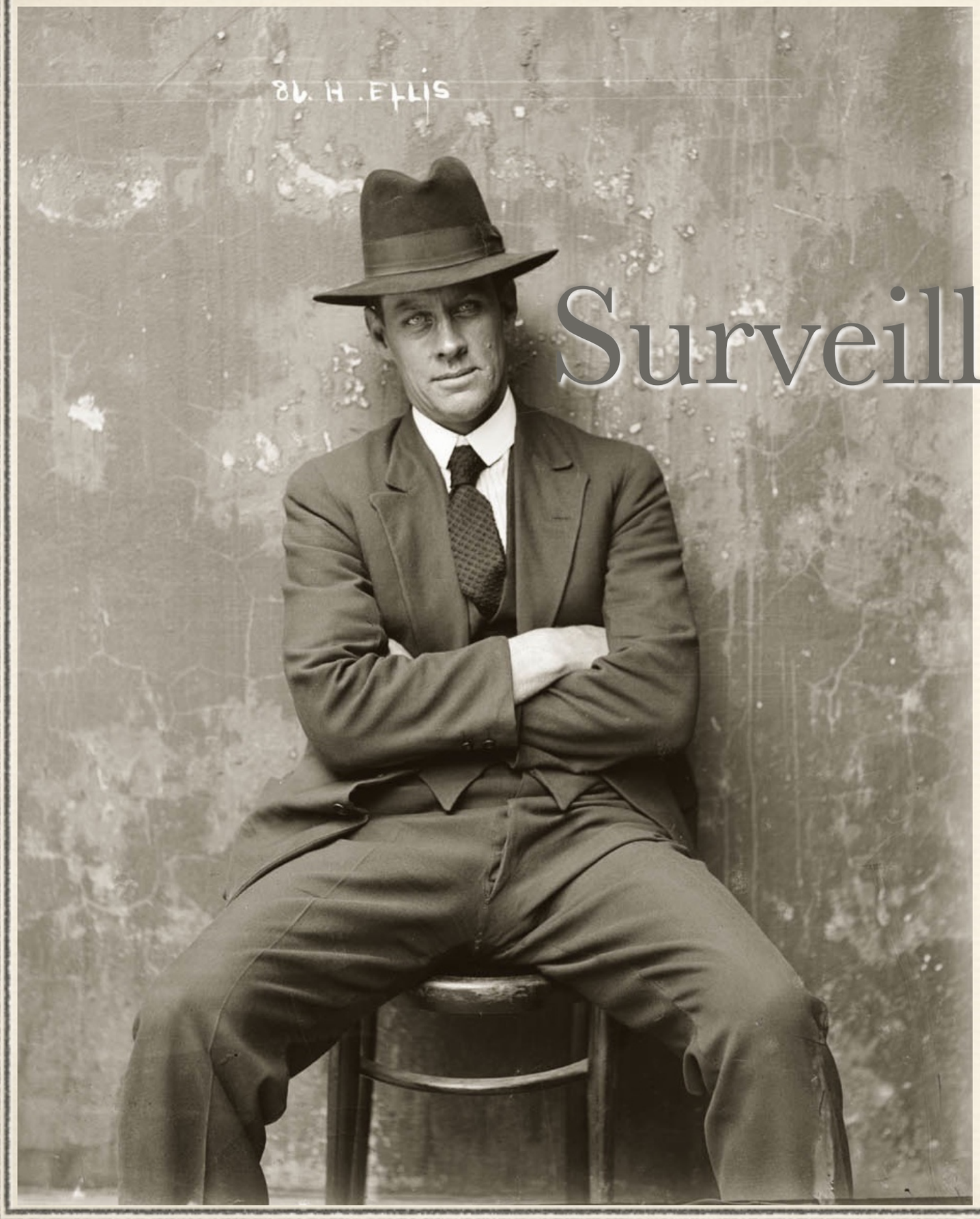
- Intel Lingo: penetrations
  - Recruited
  - Inserted
- Most serious threat

HUMINT is the biggest threat. Many sources, from forcing someone to “turn state’s evidence”, to undercover operation, to recruiting someone in place/defections... lulzsec’s collapse ultimately stems from a single individual leaving Anonymous and dumping IRC logs in public.

Technical Monitoring

- Wiretaps, etc
- Trojans and monitoring software
- Video / audio surveillance
- An increasing threat
  - See: media reports of legal trojans

FinSpy, etc.



Surveillance

- Passive observation from local population
- Dedicated active surveillance teams
- Not really a threat for hackers or professional thieves

Media Exposure

- Media coverage creates an OSINT footprint
- Can be dangerous for hackers
- Raises profile which draws adversarial attention

Contributing Factors

Factors that contribute to the groups CI strengths and vulnerabilities.

- Organizational structure
- Controlled territory
- Popular support
- Adversarial capabilities
- Resources

Organizational Structure

- Hierarchical vs. Flat
  - Flat can react faster
  - Hierarchical can enforce good practices
  - Flat leads to poor compartmentation
  - Hierarchical increase value of high level penetrations

- Tight vs. Loose
  - Loose, each node has a unique CI signature, harder to attack efficiently
  - Tight, can enforce CI discipline better
  - Loose, can have poor practices and CI resources
  - Tight can be rigid, introducing systemic CI vulnerabilities

Tightly controlled organisations react slowly and can develop rigid CI practices. This means they're exploitable.

- Area safe from adversarial intelligence gathering
- Reduces incentives to develop robust CI posture

We'll see that later, with China and Russia.

Popular Support

- Active support from the population
  - Housing, food, etc
- Passive support from the population
  - Don’t report activity to the adversary

Not really an issue for hackers, but thieves faced a hostile population.

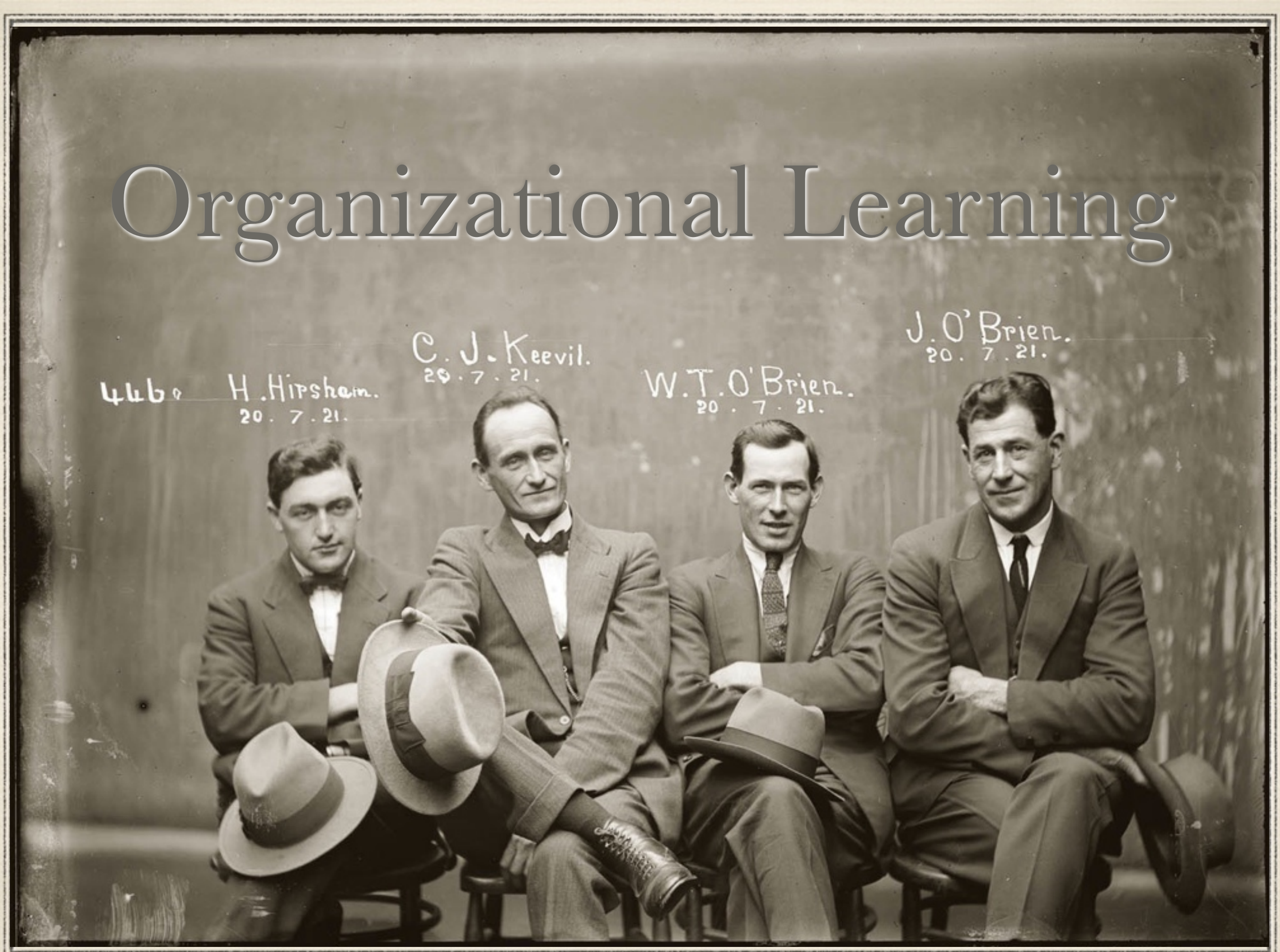
Adversary's Capabilities

- Highly capable adversary
  - Strong intelligence capabilities
  - Experienced and knowledgeable
- Low capability adversary
  - Floundering reactionary moves that are ineffective and make people angry

Resources

- Adversarial resources available for
  - Performing intelligence gathering
  - Analysis
  - Follow up actions
- Agency resources for counterintelligence
  - Dedicated CI team(s)

Organizational Learning



The way that adversarial groups learn and adjust to each other's behaviour is well studied. It is a subset of Organizational Learning -- Competitive adaptation.

Competitive Adaptation

The way these factors and processes interact is called competitive adaptation, as two adversarial groups learn from and adjust to each other's strengths and capabilities

Adverse environments breed stronger actors

Competitive Adaptation

- Organizations are superior to individuals
  - Can afford some losses and still recover
  - Deeper experience base to draw from (more *metis*)

- Setbacks lead to sense-making and recovery
  - Damage Assessments
  - Adaptive Denial

Setbacks - flaps in “Intel Speak”

Perfectly suited for their time, failed to exhibit adaptive denial and learn from competitive adaptation. They were darwinialy selected out of modern society. The lesson here for hackers is simple, either adapt where the thieves didn't or enjoy your fading golden years...

Professional Thieves

- Historical class of professional grifters
  - From 1890s to 1940s in America
- Self identify as thieves (honorific)
  - Thieve argot used to demonstrate membership
  - A large community of practice

Thieves

- Con men
  - Long con, short con
- Cannons (pickpockets)
- Boosters (shoplifters)

Organizational Structure

- Flat
- Loose
- Small “mobs” with great indivudual variation

Autocratic groups survive better than democratic groups in the face of adversarial competition

Controlled Territory

- Operating inside “fixed” towns
- Small meeting rooms

Popular support

- None
- Relied on high level penetrations of law enforcement apparatus

Professional Thief Assets

- Core skill was “larceny sense”
  - Experience derived cunning
- Access to fixers and fences
- Social network with memory for vetting members

Example tale of two thieves in boosting from a store. Thief A doesn’t get the alert from B, has item in suitcase already, sees shopkeeper, approaches and demands to see the manager. Is taken to manager, while B collects suitcase and leaves. Thief A is then confused, and walks out.

Rules for effective thievery

- Steal an item at a time
  - Stash it at a drugstore or restaurant
  - Mail it back home to a friend
    - Never keep it at home / in car
- Never grift on the way out

Rules, cont.

- Never draw attention to a working thief
- Never fail to draw attention to an adversarial threat
- Failsafe triggers to indicate problems, i.e. arrest

Lots of codes and signs – “nix” for coppers around, changing the conversation to prevent people

– always punctual to meetings, only reason to be late is arrest – mob will break up
– always call someone at fixed time at end of day, on failure they assume arrest and search

- Strict rules against informants (“rats”)
  - Violent retaliation against “rats” was sanctioned

“A professional thief will never say anything dangerous, and someone who is not a professional thief doesn’t know anything dangerous to say”

- Heavy investment in *fixers* to limit handle problems
- Little/No adaptive denial capabilities
  - Adversary maintained fixed capabilities
  - No competitive adaptation

After the adversary changed their game, lost the corruption and the “old style police work”, the professional thieves day’s were numbered. The environment became too hostile to support them in number.

Hackers

Organizational Structure

- Flat hierarchy
  - No commanders
- Loose group structure
  - Individuals pool resources, but act on their own

Controlled Territory

- Nation state protected hackers
  - Russia, China, etc.
  - Political protection: e.g. USA hacking Iran
- Secure private servers and channels
  - Unmonitored information transfer

Popular Support

- Not relevant
  - Cyberspace is not a “space”
  - Support requires knowledge
    - Who, what, etc.

Denial, Insight, Manipulation

Basic Denial

- Vetting of members
- Pseudonymity
- Limited compartmentation
  - Internal to a group
  - But.. gossip spreads far and fast

Adaptive Denial

- Limited sensemaking from colleagues' busts
- Over reliance on technical protections
- No case, ever, of a hacker penetration of LEO
  - Resulting in actionable intel to adapt

Covert Manipulation

- Occasional poor attempts at framing others
  - ProFTP AcidBitches hack
- Nation state level, certainly happens
  - False flag attacks
  - What is the cost of a VPS in Shanghai?

Hacker Community of Practice

- Informal community
- Social groups connected via social mediums
- Sharing of *metis* via formal and informal means
  - Zines, papers, blogposts, chats

Communities of Practice

- Three main hacker communities
  - English
  - Russian
  - Chinese
- Clustered by language of information exchange

Communities of Practice

- Operate inside controlled territory
  - Russian
  - Chinese
- Operate in hostile environment
  - English

Interesting that 2/3 communities are operating in controlled territory, where they have carte blanche to
operate, provided they avoid antagonizing the local authorities.

Comm of P. CI

- Controlled territory provides protection against adversarial intelligence collection
  - Discourages robust operational security practices
- Hostile environments force adaptation
  - Darwinian selection

Favorable elements in any operational situation should be taken advantage of, but not by relaxing vigilance and security consciousness.

Soviet doctrine on clandestine operations

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol9no1/html/v09i1a06p_0001.htm

Learning Disabilities

- Hacker communities of practice have severe learning disabilities
- Incurious about why colleagues got busted
- No lessons learned
- No damage assessment

Learning Disabilities

- Hacker groups are too compartmented for info sharing
  - Not compartmented enough to prevent intelligence collection

Lessons Learned

Critical Secrets

- Identity
- Operational secrets
  - When
  - How

These are the things that hackers most need to be concerned about.

Hacker CI

- Focus on Basic Denial
- Create virtual controlled territory
- Political cover for hacking

Conclusion

Adapt or die

Thank you.